PBMA-SSL
Secure Work Groups

New User Authentication And Activation Plan (NUAAP)

Prepared for the

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Report No. 0190602.12.004

Revision 0

March 31, 2004

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose

The Process Based Mission Assurance Secure Socket Layer (PBMA-SSL) application is designed to provide users with secure collaborative Work Groups using a validated method of strong user authentication. This tool enables the sharing of information deemed as sensitive/critical data such as Source Evaluation Board (SEB) data, as well as information governed under the International Traffic Arms Regulated (ITAR) or Export Administration Regulations (EAR) laws. The PBMA-SSL operates behind the NASA Glenn Research Center (GRC) firewall. The Work Groups are designed to organize information, manage documents, share schedules and facilitate efficient project team collaboration, all in a browser-based environment.

1.2 Roles

1.2.1 PBMA Work Group Originator

The Originator of the Work Group is the initial Work Group Administrator. The Originator is the data owner, who approves their data to reside in a Work Group. The Originator may not want to administer the Work Group and may assign other members of the Work Group to fill that role. The Originator will be the conduit for all password resets (reference Section 4).

As the data owner, the Originator assumes responsibility for all information posted to the Work Group.

If the Work Group will contain ITAR/EAR or ACI information, the Originator must fill out Appendix A – National Agency Check Verification. The Originator is also responsible for verifying their Member's ability to access ITAR/EAR data (keeping in-line with Code I requirements).

Reference NPR 2190.1 for NASA's current ITAR/EAR policy.

Note: ITAR/EAR data should not be accessed from a user's home PC.

1.2.2 PBMA Work Group Administrator(s)

SSL Work Group Administrator(s) are responsible for the maintenance of the Work Group site. This maintenance includes performing all administrative functions such as managing Work Group membership and access, updating general information, and review of information, content, and site activities to ensure compliance to NASA policies

and the PBMA-SSL Charter. Even if the Originator maintains control over the administration of the Work Group, a back up Administrator is prudent.

While the Work Group Administrator can perform membership and access functions, only the Originator can perform these functions for Work Groups containing ITAR/EAR or ACI data.

1.2.3 PBMA-SSL Work Group Members

The PBMA-SSL Work Group Members are the end-users of the Work Group site.

1.2.4 PBMA-SSL Technical Support

PBMA-SSL Technical Support is comprised of PBMA-SSL Information Technology (IT) personnel, who are responsible for maintaining the backbone of the PBMA network and Web site application, and the PBMA-SSL Help Desk, which is the primary interface between of the PBMA-SSL IT personnel and Work Group Administrators. It may also include other application support personnel, when needed. For the purpose of the New User Authentication and Activation Plan, all support functions are generally referred to as PBMA-SSL Technical Support.

2 SECURITY PRACTICES

In order to protect access to a Work Group, and the information contained therein, all members and support personnel must take responsibility for protecting login information.

- Never transmit user name or password by e-mail, fax, instant messaging, pager, or other electronic means. *User name and password will always be provided verbally, once the user's secret question has been correctly answered.*
- Never record login information in an unprotected location - electronic or physical, where unauthorized individuals can access it.
- Passwords must be a minimum of eight characters. The eight characters will contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, and special characters.
- Passwords must be changed every 90 days.

In support of these security standards, certain functions have been disabled in the PBMA-SSL application. They include, but are not limited to:

- The Live Chat functionality
- Community Messenger (Instant messaging tool)
- The option of selecting the "Remember me" function on the login page.

Work Group Originators, in certain unique situations, may be given Founder status within the PBMA-SSL application. This status permits modification of Work Group specific security settings. Founders must take extreme care in enforcing baseline requirements:

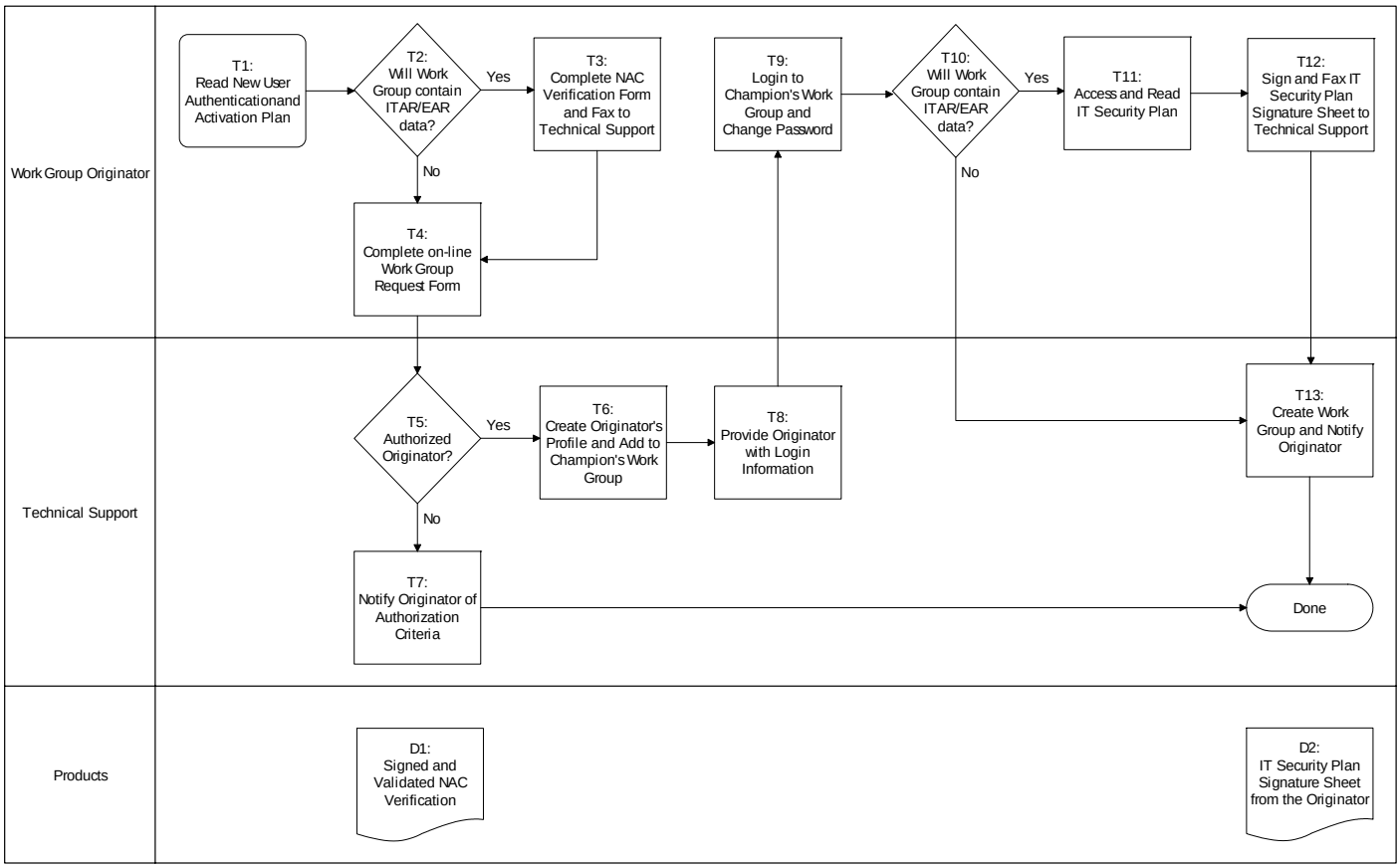
- Under Administration → Community Security, do not alter these settings. The default settings should not be altered from their current configuration.
    - Work Groups that contain ITAR/EAR or ACI data shall always be "Private" – new Members must be invited and approved by a Work Group Administrator in order to join the group. It would be prudent for the Originator to maintain complete control of membership functions in Work Groups containing ITAR/EAR or ACI data.
    - All remaining Work Groups shall be "Restricted" – new Members can be invited by a current Member, or approved for membership by a Work Group Administrator.
    - In rare instances a Work Group may be "Open" by special request only.

Work Group Administrators are responsible for ensuring that membership is limited to individuals with a legitimate need to access their Work Group. However, final membership authority will always reside with the Work Group Originator. Good security practices include:

- Verifying who is requesting membership and their need for such membership.

- Removing Inactive Users. Note: If the member to be removed has been designated as an Administrator, Technical Support must be notified to complete the removal process.
- Deleting members who no longer require or are no longer involved in the process or activity supported by the Work Group.
- Request site deactivation at conclusion of Work Group activity.

3 PROCESS FOR ACTIVATING A NEW WORK GROUP



TASKS

T1. *Read the NUAAP, which contains the SSL Communities of Practice (CoP) Charter:* Work Group Originator reads the PBMA SSL NUAAP to become familiar with the purpose of the Work Groups and the responsibilities associated with them.

T2. *Determine if Work Group will contain ITAR/EAR data.*

T3. *Complete NAC Verification form and Fax to Technical Support:* Fax the completed NAC verification form (Appendix A) to Technical Support @ (440) 962-3098.

T4. *Complete on-line Work Group Request Form:* Request a new Secure Work Group through the PBMA KMS Web site (http://pbma.hq.nasa.gov/swg).

T5. *Confirm Originator's Authorization?:* Determine if the Originator is authorized to request a new Work Group.

T6. *Create Originator's Profile and Add to Champion's Work Group.*

T7. *Inform Originator of Authorization Criteria:* If the Originator is not authorized to direct the activation of a new Work Group, explain who is and suggest they attempt to find a sponsor within that group.

T8. *Provide Originator with Login Information:* Technical Support provides the Originator's user name and initial password, and the Champion's site URL.
T9. *Log into the Champion's Work Group and Change Password:* Originator logs into the site and completes user profile information including changing his or her password.
T10. *Determine if Work Group will contain ITAR/EAR data.*
T11. *Access and Read the PBMA-SSL IT Security Plan (Report No. 0190602.12.007):* Once the Originator logs into the Champion's Work Group, they must access and read the IT Security Plan.
T12. *Sign and Fax IT Security Plan:* The Originator, as the prospective Work Group Data Owner, indicates acceptance of the plan by signing the plan's concurrence sheet.
T13. *Create Work Group and Notify Originator:* Originator will be notified by Technical Support once their Work Group is created. The system utilizes single sign-on (SSO) so all subsequent groups will use the same userid and password.

DELIVERABLES

D1. *Signed and Validated NAC Verification*.
D2. *IT Security Plan Signature Sheet from Originator*.

3.1 Read Secure Work Group NUAAP

The New User Authentication and Activation Plan (NUAAP) contains the Work Group Charter, basic rules and procedures.

Note: PBMA SSL Program Management reserves the right to deny requests for activation of any Work Group, or to delete any existing Work Group, that does not comply with the intent of the PBMA SSL CoP Charter.

3.2 Approvals Required

The PBMA SSL Work Groups are available to all NASA and contractor personnel, industry partners and academia. All Work Group Originators are required to submit proof of United States citizenship via a NAC.

3.3 Accessing the IT Security Plan

Once an Originator is approved, their profile is created and added to the Champion's Work Group where access to the IT Security Plan is made available. The Champion's Work Group is for Originators only and will have information that pertains only to

Originators. Technical Support will phone the Originator with their newly created user name and password and URL for the Champion's Work Group. The Originator must then login and change their password from the one provided by Technical Support to one of their choosing. This user name and password is universal for all Work Groups in which the Originator will have membership. This application takes advantage of single sign-on (SSO).

Note: Users of the Secure Work Groups will only have one account. One userid and one password will be used for access to all Secure Work Group.

Once the Originator gains access to the Champion's Work Group, they must access and read the Information Technology (IT) Security Plan then sign the signature sheet. By signing this plan, the Originator gives consent as the Data Owner for their sensitive information to reside on the Secure Work Group. The signature sheet, with the Originator's original signature, must be provided to Technical Support. In order to expedite the activation process, a facsimile is recommended. The SSL Work Group cannot be activated without the Originator's signature on the IT Security Plan.

3.4 Work Group Request

Note: It is the responsibility of the Originator to customize Work Group settings, approve individuals for membership, and upload any initial content.

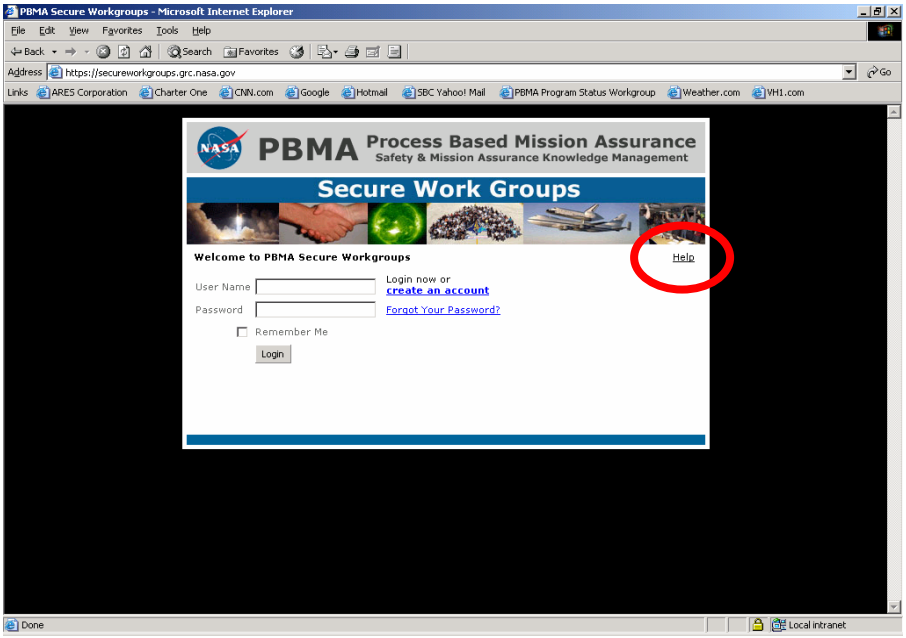
The Originator must provide the following information when applying for a Secure Work Group via the on-line form (http://pbma.hq.nasa.gov/swg):

- Name
- Title
- NASA Center affiliation
- Organization
- Work Phone
- E-mail Address
- Name of Work Group
- Summary Description of Work Group (1-2 Sentences)
- Detailed Description/Purpose of the Working Group (1-2 Paragraphs)
- Secret Question or Phrase
- Response to Question or Phrase

Since passwords will only be issued verbally, the secret question or phrase and response are for verification purposes.

4 GETTING HELP

Technical Support is available when the information provided in this document and online help proves insufficient. All support issues will be routed to the Help Desk via the "Help" link found at https://secureworkgroups.grc.nasa.gov as seen below.



As an example, the responsibility of managing password resets and reissues will belong to PBMA-SSL Technical Support. If a user needs their password reset, they must choose the "Reset Password" option from the scroll down menu. Once the user submits their request to the Help Desk, Technical Support will create a new random password and provide it to the Work Group Originator.

Note: It is the Work Group Originator's responsibility to communicate password changes to their members.

Information to have available when PBMA-SSL Technical Support contacts you:

- Name
- Work Group
- Response to Secret Question

Technical support can only be contacted via the Help Menu. All requests will be handled as quickly as possible to maintain optimal operation of the Work Groups. Any requests received outside of standard operating hours will be handled as soon as possible the following business day.

5 PROCESS FOR INCREASING DISK STORAGE SPACE

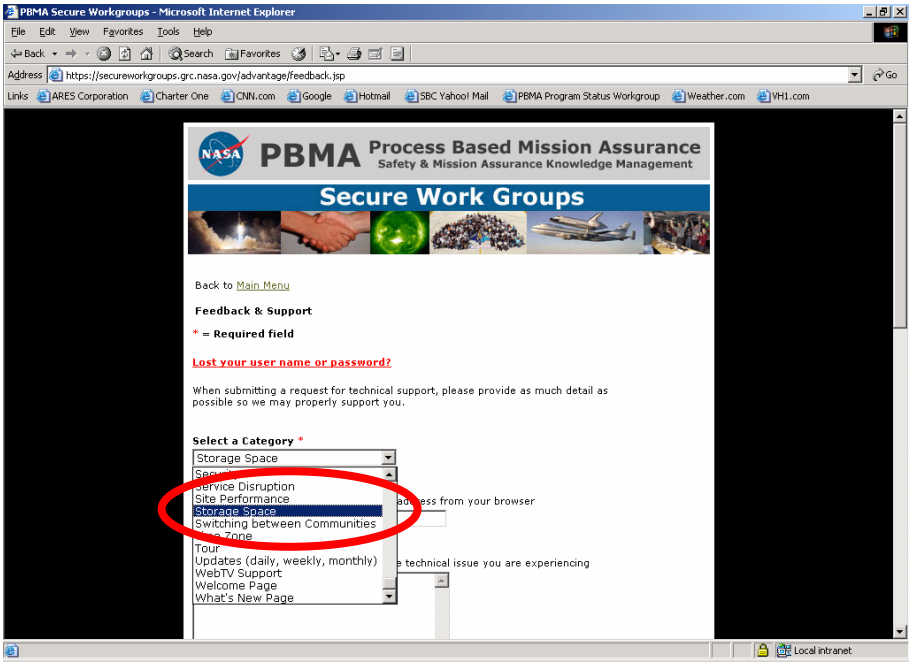
5.1 Requesting Additional Disk Storage Space

5.1.1 Approvals Required

Any Work Group Originator or Administrator may request an increase in the storage capacity of a Work Group for which they have responsibility.

5.1.2 Submitting the Request

When requesting additional storage capacity, go to the Help Menu and submit request to the Help Desk as seen below.



Requests are often processed on the day that they are received; however, you should allow five (5) business days.

6 PROCESS FOR DISCONTINUING A WORK GROUP

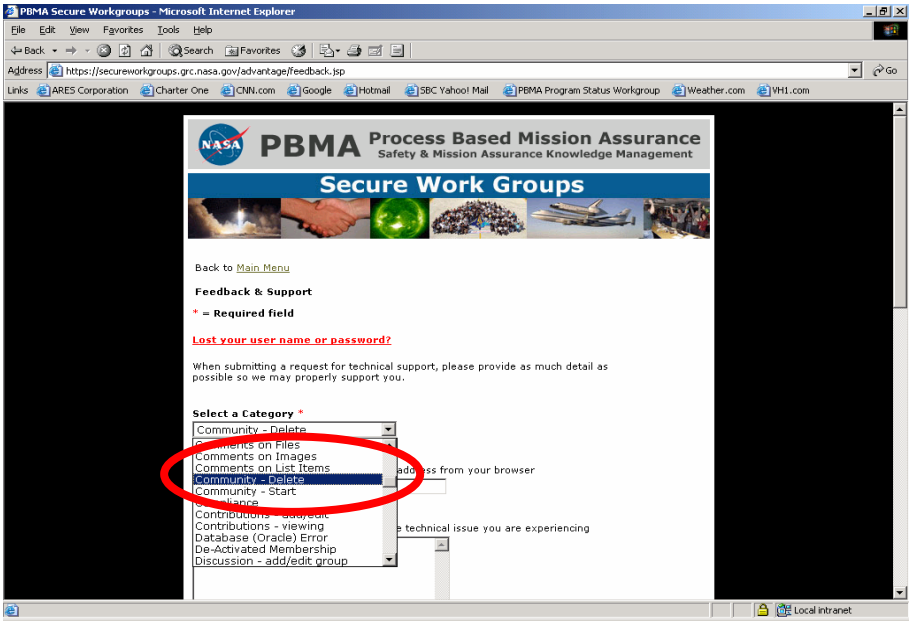
If a Work Group is no longer necessary, it will need to be deleted. Requesting deletion of the Work Group is the responsibility of the Work Group Originator.

6.1 Notify Members of Pending Deactivation

The Work Group Administrator must notify all Work Group Members that the site will be deleted. This can be accomplished by posting an announcement on the Work Group site itself, by sending an e-mail to the entire membership, or both. The message should include the expected deletion date and a reminder to Work Group Members that any data stored on the site will become unavailable following deletion.

6.2 Submitting the Request

The request to discontinue a SSL Work Group must be submitted to the Help Menu and submit request to the Help Desk as seen below.



Requests are often processed on the day that they are received; however, you should allow five (5) business days.

7 TECHNICAL SUPPORT INFORMATION

Contact for PBMA-SSL Technical Support:

E-mails should be addressed to mailto:pbma_workgroup@arescorporation.com

Standard operating hours of PBMA-SSL Technical Support is Monday through Friday 8:00 AM to 5:00 PM EST. Technical Support will observe the same holidays as NASA.

8 PBMA SECURE WORK GROUPS CHARTER

NASA Process Based Mission Assurance
Secure Work Groups (PBMA-SSL)
General Charter

Secure Work Groups:

Secure Work Groups are available as an enhanced functionality of Process Based Mission Assurance (PBMA). These Secure Work Groups provide multi-dimensional, collaborative functionality to support the NASA Safety and Mission Assurance community, individual program/project teams as well as formal and informal groups of subject matter experts.

Membership is limited to those individuals involved in making NASA programs and projects successful, including contractors, industry partners, and academia. Membership in the community is predicated on the notion of reciprocity and sharing of knowledge as well as responsiveness to the needs and inquiries of the community

Legal/Security Ground Rules

Promote knowledge sharing and foster group interaction while observing basic cautionary measures:

- No classified information.
- Work Group Members must be verified by their Work Group Originator.

For additional information on these topics please contact:

Your Center Export Administrator or Export Counsel, listed at:
http://www.hq.nasa.gov/office/codei/nasaecp/

Or access the following NASA documents:

OMB Circular A-130
NPR 2190.1: NASA Export Control Program
NPD 2110.1: Foreign Access to NASA Technology Utilization Material
NPD/NPG 2800.1: Managing Information Technology
NPD/NPG 2810.1: Security of Information Technology
NPG 1620: Security Procedures and Guidelines
NIST 800-53: Recommended Security Controls for Federal Information Systems

Work Group Originator Requirements

- Review information content of the community space to assure the Work Group is not violating NASA policies regarding information security and technology transfer
- Manage and control Work Group membership and access
- Notify new members that join the Work Group outlining their responsibilities
- Prepare concise Work Group statement of purpose (two or three sentences)
- Prepare Work Group charter (two or three paragraphs)
- Visit community space on a regular basis and add new information, update or remove old information
- Mentor new members in the general functioning of the specific community

New Work Group Originators will be invited to join the *SSL Champions Work Group*, a Work Group for additional guidance and support from other Work Group Originators and the PBMA-SSL development team.

Work Group Members

- Activities that will not be tolerated and are grounds for termination of participation include:
  - Using the community space for unprofessional means, i.e., spamming, flaming, etc.
  - Violating the NASA policies regarding information disclosure
  - Violating the NASA policies regarding security and personnel safety
- Review the community-specific charter and pertinent literature including postings to the community space
- Biographical sketch (and potentially a digital photo) for posting in the community space

Work Group Support Activity

- Periodic workshops will be conducted providing lessons learned and best practice case studies for Work Group managers
- General metrics such as number of members, last date of activity within a Work Group, etc., will be collected and reported to PBMA-SSL management

Appendix A – National Agency Check Verification

NAC Verification Form for PBMA-SSL Work Group Originator

PLEASE write legibly and read thoroughly.

All Secure Work Groups require that you must have the approval signature of your appropriate Center's security personnel. Requests should be delivered to PBMA-SSL Technical Support, c/o ARES Corporation, 21000 BrookPark Rd., MS 501-4, Cleveland, OH 44135, or Fax to (440) 962-3098.

Name _____ Title _____

Center _____ Work Phone _____

Organization _____ E-mail Address _____

You are requesting a secure work group that will be approved for sensitive but unclassified data up to ITAR/EAR data.

You agree that unauthorized use of the computer accounts and computer resources to which you are granted access may be a violation of NPG 2810.1 and NPR 2190.1. You will make every effort to protect your account(s) from unauthorized access and will not knowingly permit access by others. Misuse of your assigned accounts and by accessing others' accounts without authorization is not allowed. You understand that these resources are subject to monitoring and recording by the Glenn Research Center to detect unauthorized use in accordance with NPG 2810.1. You further understand that failure to abide by these provisions may constitute grounds for termination of account access, administrative action, and/or civil or criminal liability as set forth in NPG 2810.1, NPR 2190.1 and other applicable laws and regulations.

All users must follow these additional rules:

- No Classified Information may be posted.
- Include only information related to official NASA business.

I certify that I am a United States citizen and have had a National Agency Check (NAC) performed.

I, _____ hereby certify that I understand, and upon the granting of access to the Web server shall comply with all above statements.

_____ _____
Work Group Originator Signature Date

_____ _____ _____
Center Security Representative Signature Phone Number Date

For Internal Use Only

_____ _____
Verification of Citizenship and NAC by Technical Support **Date**